**K. J. Somaiya College of Engineering, Mumbai-77**

**Department of Computer Engineering**

**Batch: A2 Roll No.:**

**Experiment No. 3**

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of the Staff In-charge with date**

|  |  |
| --- | --- |
|  |  |
| **Title:** | **Merkle Tree** |

**Objective:**

**Expected Outcome of Experiment:**

|  |  |
| --- | --- |
| **CO** | **Outcome** |
|  |  |

**Books/ Journals/ Websites referred:**

**Implementation Details:** *import hashlib*

*n = int(input('Enter number of transactions in exponent of 2 : ')) t = int(input('Enter number of transactions per block, in exponent of 2 : '))*

*def Nonce(string): nonce = 0 while(True):*

*new\_string = string + str(nonce) result =*

*hashlib.sha256(new\_string.encode("utf-8"))*

*# print(result.hexdigest())* *nonce += 1 if(result.hexdigest()[0:4] == "0000"):* *return result.hexdigest(), nonce*

Department of Computer Engineering BCT Sem-VI (Honors) – July-Nov 2023 Page - 1

**K. J. Somaiya College of Engineering, Mumbai-77**

**Department of Computer Engineering**

*def MerkleRoot(n): transArr=[0 for i in range(2\*\*n)] for i in range(2\*\*n): transArr[i]*

*= hashlib.sha256(str(input('Enter transaction message : ')).encode()).hexdigest()*

*for j in range(n):*

*for i in range(0,2\*\*n,2\*\*(j+1)):*

*# print(j,i) # print(transArr)*

*t = (transArr[i]+transArr[i+(2\*\*j)])*

*# print(t)*

*transArr[i] = hashlib.sha256(str(t).encode()).hexdigest()*

*# print(transArr) return transArr[0]*

*def Block(n,p):*

*prevBlockHash = "0000" for x*

*in range((2\*\*n)//(2\*\*p)):*

*currRoot = prevBlockHash + MerkleRoot(p)*

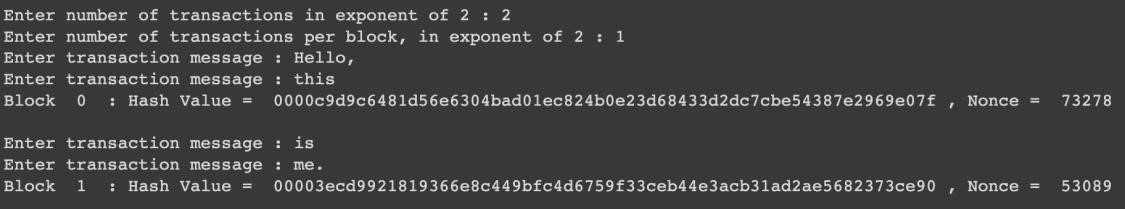
*currBlockHash, nonce = Nonce(currRoot)*

*# currBlockHash = hashlib.sha256(currRoot.encode()).hexdigest() print("Block*

*",str(x)," : Hash Value = ",str(currBlockHash),", Nonce =*

*",str(nonce),"\n")* *prevBlockHash = currBlockHash*

*Block(n,t)*



**Conclusion:-**

In this experiment, we learnt about how to build a working model of a private blockchain. We did this using the principle of nonce, Merkle Tree Root and transactions, taking in as input the number of total transactions and number of blocks, and then printing the hash value of each block along with the nonce.

Department of Computer Engineering BCT Sem-VI (Honors) – July-Nov 2023 Page - 2